SECTION 230 OF THE COMMUNICATIONS DECENCY ACT:
A BLUEPRINT FOR REFORM

By

Andrew P. Bolson, Esq.

June 2019

Section 230 of the Communications Decency Act was signed into law by President Clinton on February 8, 2016.

For some perspective:

1996	***2019***
20 million Americans had access to the Internet	312 million Americans access the Internet
AOL was the world's largest Internet provider	In 2015, AOL sold to Verizon for $4.4 billion
Google did not exist	Google is the fourth most valuable company with a market capitalization nearing 1 trillion dollars
Mark Zuckerberg was 12	Mark Zuckerberg is 34, has 2 children and been the CEO of Facebook since 2004
100,000 websites existed	1.94 billion websites exist
On average, Americans spent less than 30 minutes a month on the Internet	On average, Americans spend 24 hours on the Internet per week.

The Internet has changed, but the law has not.

TABLE OF CONTENTS

INTRODUCTION

In 1996, at the dawn of the Internet Age, Congress passed Section 230 of the Communications Decency Act ("Section 230"), a seminal law that immunized websites and service providers for the content posted on their platforms by third-parties.[1] Without civil immunity, Facebook, Twitter and the like could be held liable for every post uploaded to their platforms, a result that would likely lead to the wholesale removal of content by platforms in order to avoid liability.[2] It is not a stretch to suggest that Section 230 is largely responsible for the social media industry, which has transformed our world for better and worse.[3]

The benefits to society by virtue of Section 230 must be balanced against the considerable costs that the law creates to victims of online abuse. As a result of Section 230's immunity, abusive and harassing content has been allowed to proliferate online without websites hosting such content facing any financial consequence for their role in perpetuating the abuse. For example, immunity has been upheld for online platforms hosting terroristic content, for spreading nonconsensual pornography, for allowing users to conduct illegal activities, and for doing nothing when notified about online impersonation.[4]

It is unlikely that any law could eliminate all forms of online abuse. That being said, current law relies upon self-regulation and the hope that websites, even with immunity, will act

---

[1] *See* Communications Decency Act of 1996, 47 U.S.C. § 230 (2012); *see generally* JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (Cornell University Press 2019); *see also* Danielle Keats Citron and Benjamin Wittes, *The Problem Isn't Just Backpage: Revising Section 230 Immunity*, 2 GEO L. TECH. REV. 453 (2018).

[2] *See, e.g.,* Aja Romano, *A new law intended to curb sex trafficking threatens the future of the internet as we know it*, VOX.COM (July 2, 2018), https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom.

[3] As for the better, *see,* e.g., Heather Leson, *How is social media helping disaster response?*, WORLD ECONOMIC FORUM (April 6, 2016), https://www.weforum.org/agenda/2016/04/how-is-social-media-helping-disaster-response/; Melissa Tyas, *How can social media platforms support activists?*, WORLD ECONOMIC FORUM (April 6, 2016), https://www.weforum.org/2016/04/how-can-social-media-platforms-support-activists; Shannon Dosemagen, *Can social media help to save the environment?*, WORLD ECONOMIC FORUM (April 7, 2016), https://www.weforum.org/2016/04/can-social-media-help-to-save-the-environment; Isis Briones, *12 Major artists who got their start on YouTube*, TEEN VOGUE (Mar. 29, 2016), https://www.teenvogue.com/story/best-artists-discovered-on-youtube. As for the worse, *see, e.g.,* Zach Beauchamp, *Social media is rotting democracy from within*, VOX.COM (Jan. 22, 2019), https://www.vox.com/policy-and-politics/2019/1/22/18177076/social-media-facebook-far -right-authoritarian-populism; Sheera Frenkel, Mike Isaac and Kate Conger, *On Instagram, 11,696 Examples of How Hate Thrives on Social Media*, NY TIMES (Oct. 29, 2018), https//www.nytimes.com/2018/10/29/technology/hate-on-social-media.html?module=inline.

[4] Russell Spivak, *Facebook Immune from Liability Based on Third-Party Content*, LAWFARE.COM (May 23, 2017), https://www.lawfareblog.com/facebook-immune-liability-based-third-party-content; Citron and Wittes, *supra* note 1 at 466.

as "Good Samaritans." The problem is that websites that abuse their immunity are treated no differently than those actively moderating their platforms and instituting baseline protocols to prevent abuse. Reforming Section 230 to require that websites institute certain safety and procedural protocols would make a significant difference in mitigating the harms created by the Internet's worst offenders and indifferent actors.

This paper seeks to highlight some problems resulting from Section 230, both substantively and procedurally, and offers a blueprint for reform. Organized into four sections, this paper will first provide a brief overview of the history of Section 230. Next, this paper will examine existing legislation that could serve as a model for reform. Third, this paper will discuss several forms of abuse aggravated by Section 230, including online impersonation, nonconsensual pornography and doxing and proposes to condition Section 230 immunity on websites taking action to mitigate these abuses. Finally, this paper will analyze procedural impediments for victims dealing with online abuse, including anonymity, difficulty with the enforcement of court orders, complications with the issuance of subpoenas and the problem of foreign websites outside of American jurisdiction and will make recommendations to limit or remove such impediments.

Section 230 purists believe that there is a binary choice between immunity for user generated content and regulation that would cripple the Internet as we know it.[5] Such a binary choice is a fallacy. A regulatory scheme that conditions Section 230 immunity on adherence to defined protocols can offer a balanced solution, incentivizing platforms to do more to address online abuse while preserving immunity for user generated content when such protocols are followed.

[5] *See, e.g.*, *Section 230 of the Communications Decency Act*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/cda230 (last visited April 23, 2019); Issie Lapowsky, *Lawmakers Don't Grasp the Sacred Tech Law They Want to Gut*, WIRED.COM (July 17, 2018), https://www.wired.com/story/lawmakers-dont-grasp-section-230/; Derek Khanna, *The Law that Gave Us the Modern Internet – and the Campaign to Kill It*, THEATLANTIC.COM (September 12, 2013), https://www.theatlantic.com/business/archive/2013/09/the-law-that-gave-us-the-modern-internet-and-the-campaign-to-kill-it/279588/.

LEGISLATIVE HISTORY

Section 230 of the Communications Decency Act was born out of a response to *Stratton Oakmont*, a Supreme Court of New York decision issued on May 24, 1995.[6] In *Stratton Oakmont*, a securities investment banking firm sued Prodigy Services Company for statements posted on Prodigy's "Money Talk" computer bulletin board.[7] The statements included the following:

> (a) Stratton Oakmont, Inc. ("Stratton"), a securities investment banking firm, and Daniel Porush, Stratton's president, committed criminal and fraudulent acts in connection with the initial public offering of stock of Solomon-Page Ltd.;
> (b) The Solomon-Page was a "major criminal fraud" and "100% criminal fraud";
> (c) Porush was "soon to be proven criminal"; and
> (d) Stratton was a "cult of brokers who either lie for a living or get fired."[8]

The Court analyzed Prodigy's liability vis-à-vis the editorial control that Prodigy exercised over the content posted on its site.[9] According to the Court, "Prodigy held itself out to the public and its members as controlling the content of its computer bulletin boards."[10] In addition, the Court noted that "Prodigy implemented this control through its automatic software screening program, and the Guidelines which Board Leaders are required to enforce. By actively utilizing technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and 'bad taste', for example, Prodigy is clearly making decisions as to content, and such decisions constitute editorial content."[11] The Court determined that Prodigy's conscience decision to exercise editorial control over third-party content opened the company to greater liability as a publisher.[12]

The *Stratton Oakmont* decision marked a departure from existing precedent established in *Cubby, Inc. v. Compuserve, Inc.*, which held that liability for online distributors would be no

---

[6] Stratton Oakmont v. Prodigy Servs. Co., 1995 *N.Y. Misc. LEXIS* 299 (Sup. Ct. N.Y. May 24, 1995).
[7] *See id.* at *1.
[8] *Id.* at *2. Ironically, the statements that formed the basis for the defamation lawsuit eventually came true. Soon after the Court's decision Stratton Oakmont was banned from the brokerage industry and closed operations. In 1999, Stratton Oakmont, Inc.'s executives, Jordan Belfort and Daniel Porush, pled guilty to securities fraud. *See* Edward Wyatt, *Stratton Oakmont Executives Admit Stock Manipulation*, N.Y. TIMES (Sept. 24, 1999), http://www.nytimes.com/1999/09/24/business/stratton-oakmont-executives-admit-stock-manipulation.html. The story of Jordan Belfort and Stratton Oakmont would later be made into the Wolf of Wall Street, starring Leonardo DiCaprio. WOLF OF WALL STREET (Paramount Pictures 2013).
[9] *See Stratton Oakmont*, 1995 *N.Y. Misc. LEXIS* at 7.
[10] *Id.* at 10.
[11] *Id.* (internal citations omitted).
[12] *See id.* at *13.

different than traditional content distributors, such as "news vendors, book stores, and libraries."[13] In *Cubby*, Compuserve was sued for allegedly defamatory statements that were published on a forum available through its online service, Rumorville.[14] Traditionally, liability for content distributors applied only if the content distributor knew or had reason to know of the allegedly defamatory statements.[15] Applying these traditional principles, the Court found that because CompuServe had no knowledge of or reason to know of the allegedly defamatory statements, it was not liable for any statements posted on its site.[16]

By refusing to follow *Cubby's* precedent, the *Stratton Oakmont* decision opened the door for online content distributor liability based upon the level of the distributor's editorial control of the material posted on their websites or online forums.[17] The potential for distributor liability imposed by *Stratton Oakmont* raised concerns that, in response to the decision, Internet companies would stop monitoring content in order to avoid potential liability.[18] To alleviate this concern, Representatives Christopher Cox and Ron Wyden sponsored a bill entitled, "Protection for Private Blocking and Screening of Offensive Material"[19] Barely two months after *Stratton Oakmont* was decided, on August 4, 1995, Congressman Cox spoke on the floor of the House of Representatives and expressed the need for legislation to address the problem created by the *Stratton Oakmont* decision.[20] Congressman Cox stated in part:

> [. . .]
>
> The Internet is a fascinating place and many of us have recently become acquainted with all that it holds for us in terms of education and political discourse.
>
> [. . .]
>
> As a parent of two, I want to make sure that my children have access to this future and that I do not have to worry about what they might be running into on line. I would like to keep that out of my house and off my computer. How should we do this?
>
> Some have suggested, Mr. Chairman, that we take the Federal Communications Commission and turn it into the Federal Computer Commission, that we hire even more bureaucrats and more regulators who will attempt, either civilly or criminally, to punish

[13] *Cubby, Inc. v. Compuserve, Inc.*, 776 *F. Supp.* 135, 139 (S.D.N.Y. 1991).
[14] *Id.* at 138.
[15] *Id.* at 139.
[16] *See id.* at 141.
[17] *See id.*
[18] 141 CONG. REC. H8468 (daily ed. Aug. 4, 1995) (statement of Rep. Cox.)
[19] *Id.*
[20] *Id.*

people by catching them in the act of putting something into cyberspace.

[. . .]

Mr. Chairman, what we want are results. We want to make sure we do something that actually works. Ironically, the existing legal system provides a massive disincentive for the people who might best help us control the Internet to do so.

I will give you two quick examples: A Federal court in New York, in a case involving CompuServe, one of our on-line service providers, held that CompuServe would not be liable in a defamation case because it was not the publisher or editor of the material. It just let everyone come onto your computer without, in any way, trying to screen it or control it.

But another New York court, the New York Supreme Court, held that Prodigy, CompuServe's competitor, could be held liable in a $200 million defamation case because someone had posted on one of their bulletin boards, a financial bulletin board, some remarks that apparently were untrue about an investment bank, that the investment bank would go out of business and run by crooks.

Prodigy said, "No, no; just like Compuserve, we did not control or edit that information, or could we, frankly. We have over 60,000 of these messages each day, we have over 2 million subscribers, and so you cannot proceed with this kind of a case against us."

The Court said, "No, no, no, no, you are different; you are different because you are a family friendly network. You advertise yourself as such. You employ screening and blocking software that keeps obscenity off your network. You have people who are hired to exercise an emergency delete function to keep that kind of material away from your subscribers. You don't permit nudity on your system. You have content guidelines. You, therefore, are going to face higher, stricker [sic] liability because you tried to exercise some control over offensive material."

Mr. Chairman, that is backward. We want to encourage people like Prodigy, like CompuServe, like American Online, like the new Microsoft network, to do everything possible for us, the customer, to help us control, at the portals of our computer, at the front door of our house, what comes in and what our children see. This technology is very quickly becoming available, and in fact everyone one of us will be able to tailor what we see to our own tastes.

[. . .]

> Mr. Chairman, our amendment will do two basic things: First, it will protect computer Good Samaritans, online service providers, anyone who provides a front end to the Internet, let us say, who takes steps to screen indecency and offensive material for their customers. It will protect them from taking on liability such as occurred in the Prodigy case in New York that they should not face for helping us and for helping us solve this problem. Second, it will establish as the policy of the United States that we do not wish to have content regulation by the Federal Government of what is on the Internet, that we do not wish to have a Federal Computer Commission with an army of bureaucrats regulating the Internet because frankly the Internet has grown up to be what it is without that kind of help from the Government. In this fashion we can encourage what is right now the most energetic technological revolution that any of us has ever witnessed. We can make it better. We make sure that it operates more quickly to solve our problem of keeping pornography away from our kids, keeping offensive material from our kids, and I am very excited about it.
>
> There are other ways to address this problem, some of which run head-on into our approach. About those let me simply say that there is a well-known road paved with good intentions. We all know where it leads. The message should be from this Congress we embrace this new technology, we welcome the opportunity for education and political discourse that it offers for all of us. We want to help it along this time by saying Government is going to get out of the way and let parents and individuals control it rather than Government doing that job for us. [21]

The Cox/Wyden bill became Section 230 of the Communications Act which was passed by Congress as a part of the Telecommunications Act of 1996 on February 1, 1996 and was signed into law by President Clinton on February 8, 1996. The statute reads as follows:

> (a) Findings. The Congress finds the following:
>
> 1. The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.
>
> 2. These services offers users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.

[21] *Id.*

3. The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual property.

4. The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

5. Increasingly Americans are relying on interactive media for a variety of political, educational, cultural and entertainment services.

(b) Policy. It is the policy of the United States –

1. To promote the continued development of the Internet and other interactive computer devices and other interactive media;

2. To preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal and State regulation;

3. To encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

4. To remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

5. To ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

(c) Protection for "Good Samaritan" blocking and screening of offensive material.

1. Treatment of publisher or speaker. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

2. Civil liability. No provider or user of an interactive computer service shall be held liable on account of –

> A. Any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> B. Any action taken to enable or make available to information content providers or others the technical means to restrict to material described in paragraph (1) [subparagraph (A)].[22]

Section 230 of the CDA was passed with the best of intentions. Congressman Cox hoped that online websites would use the immunity to remove objectionable content without facing liability for doing so. Since its passage, Section 230 has been broadly interpreted, allowing websites to avoid liability even when knowing its conduct was harming its users or third-parties. Over twenty-years after the law's passage, Section 230 demands reform to achieve the goal of the drafters, namely to protect the safety of Internet users while promoting technological innovation. While Section 230's promise never fully materialized, its intent can better be achieved through the conditioning the law's grant of broad immunity.

[22] 47 U.S.C. § 230.

A BLUEPRINT FOR REFORM

In 1998, the Online Copyright Infringement Liability Limitation Act ("OCILLA") was passed as part of the Digital Millennium Copyright Act ("DCMA").[23] The same year the Children's Online Privacy Protection Act ("COPPA") was also passed into law. Both laws offer guidance for amending Section 230.

OCILLA provides conditional immunity for online service providers for copyright infringement if such providers follow certain rules, such as the removal of infringing material upon notice.[24] COPPA regulates websites that target children thirteen (13) years of age or younger and requires them to follow certain rules set forth by the Federal Trade Commissions ("FTC").[25] Regulations include the posting of a privacy policy describing the website's information collection practices, notice to parents of such practices, obtaining consent from parents for the collection of their children's information and allowing parents to review and refuse to permit further collection or dissemination of their child's information.[26] While OCILLA provides a private right of action for violations of the law, COPPA is exclusively enforced by government regulators.

An amended Section 230 should borrow from both the regulatory schemes set forth in OCILLA and COPPA. From OCILLA, this paper takes the premise that immunity should be conditional and based upon websites following certain protocols, including the honoring of court orders, the following of protocols to prevent impersonation and regulations to address anonymity. COPPA exemplifies a statute whereby an administrative body (in that case the FTC) is empowered to issue regulations to define the protocols required of websites. Section 230 requires a regulatory body that can issue regulations to set forth the conditions for which immunity would apply. Violations of such protocols should result in the elimination of immunity for the content publishers and should allow private lawsuits against the publishers of the content to proceed.

As a general matter, I believe Congress should also consider a new administrative agency whose mission would be to protect the privacy and safety of Internet users.[27] Currently, much of

---

[23] 17 U.S.C. § 512.

[24] *See id.*

[25] 15 U.S.C. § 6501.

[26] *Complying with COPPA: Frequently Asked Questions*, FEDERAL TRADE COMMISSION.GOV (last visited April 28, 2019), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[27] The United Kingdom recently proposed a White Paper that called for an independent regulator to "implement, oversee and enforce the new regulatory framework [for the Internet]." Further, "[t]he regulator will also have broader responsibilities to promote education and awareness-raising about online safety, and to promote the development and adoption of safety technologies to tackle online harms." The White Paper indicated that, "[t]he regulator will be funded by the industry in the medium term, and the government is exploring options such as fees, charges or an industry levy to put it on a sustainable footing." *See Online Harms White Paper*, HM GOVERNMENT

the administrative authority governing the Internet has been designated to the FTC. However, the FTC has a broad mandate and limited resources to dedicate to Internet governance.[28] The Internet requires its own administrative body that could be funded through taxing Internet companies who have achieved certain thresholds, either number of users or total revenue.

Notably, Mark Zuckerberg, the founder of Facebook, recently wrote an Op-Ed calling for greater regulation of the Internet. Mr. Zuckerberg wrote, "I believe we need a more active role for governments and regulators. By updating the rules for the Internet, we can preserve what's best about it – the freedom for people to express themselves and for entrepreneurs to build new things – while also protecting society from broader harms."[29]

In the future, Congress should also consider the development of a specialized division within the Federal Courts that would be tasked with resolving online disputes.[30] Specialized courts would possess judges and staff with issue expertise, could establish procedures that would streamline the issuance of subpoenas and court orders and could create an expedited discovery and trial calendar to ensure that content removal determinations are made in an expeditious manner.

53-54 (April 2019); *see generally* FRANK PASQUALE, THE BLACK BOX SOCIETY 140 – 188 (Harvard University Press 2015).

[28] Harper Neidig, *FTC says it only has 40 employees overseeing privacy and data security*, THEHILL.COM (April 3, 2019), https://thehill.com/policy/technology/437133-ftc-says-it-only-has-40-employees-overseeing-privacy-and-data-security; *see also* Tony Romm, *The agency in charge of policing Facebook and Google is 103 years old. Can it modernize?*, WASH. POST (May 3, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech/.

[29] Mark Zuckerberg, *The Internet needs new rules. Let's start in these four areas*, WASH. POST (Mar. 30, 2019), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.7c26c5b92333.

[30] It should be noted that Facebook has proposed its own independent judiciary to handle content moderation decisions. Max Read, *Facebook is going to Have a Supreme Court. Will it Work?,* NY MAG. (Jan. 30, 2019), http://nymag.com/intelligencer/2019/01/facebooks-new-oversight-board-is-a-supreme-court.html. Efforts are also underway to create a judicial body to handle content appeals over multiple platforms. *See* SOCIAL MEDIA COUNCILS: FROM CONCEPT TO REALITY, STANFORD GLOBAL DIGITAL POLICY INCUBATOR (2019), https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/gdpiart_19_smc_conference_report_wip_2019-05-12_final_1.pdf; *see also* Pasquale, *supra* note 27 at 198. The developing concept of social media courts is optimal for ensuring websites adhere to their own moderation policies. On the other hand, traditional courts remain necessary to issue subpoenas, to compel compliance with take down orders and to award monetary and injunctive relief. China, for example, has already created Internet Courts to address "business transactions, personal information and intellectual property online." *See* Jennifer Bisset, *China has an actual court dedicated to the internet*, CNET.COM (Sept. 9, 2018), https://www.cnet.com/news/china-has-an-actual-court-dedicated-to-the-internet/.

ONLINE HARASSMENT

Online harassment is a spectrum of abuse ranging from the annoying to the dangerous.[31] Broadly, online harassment is the malicious use of the Internet to do harm to another person. Specifically, online harassment includes cyber bullying, cyber stalking, doxing, online impersonation and trolling. The scale of the problem is staggering. In fact, a 2017 Pew Research study found that 41% of Americans were found to have been subjected to harassing behavior online and 18% of Americans have been subjected to more severe forms of harassment, such as "physical threats, harassment over a sustained period, sexual harassment or stalking."[32]

The impact of online harassment can be significant, with victims often experiencing problems with friends or family, reputational harm, relationship issues, financial loss, and difficulty with obtaining a job or housing.[33] This section analyzes some specific forms of online harassment, including online impersonation, nonconsensual pornography and doxing, which could be mitigated through amending Section 230.

Online Impersonation

Online impersonation or "catfishing" is when a false profile is established for "fraudulent or deceptive purposes." A 2015 report from the National Crime Prevention Council found that, "forty-three percent of teenagers have been victims of cyberbullying."[34] Of those teenagers, "nearly twenty percent were cyberbullied via online impersonation, being fooled by an impersonator into revealing personal information. Thirteen percent of victims learned that a cyberbully was pretending to be them while harassing someone else."[35] Victims of online impersonation experience significant emotional, financial and reputational harm.[36]

The dangers of online impersonation are exemplified by the case, *Matthew Herrick v. Grindr, LLC*. In that case, the plaintiff's former boyfriend used the app, Grindr, to impersonate Herrick and spread claims, including that he was, "interested in fetishistic sex, bondage, role playing, and rape fantasies and which encourage potential suiters to go to Herrick's home or

---

[31] AMANDA LENHART, ET. AL., ONLINE HARASSMENT, DIGITAL ABUSE AND CYBERSTALKING IN AMERICA, DATA & SOCIETY RESEARCH INSTITUTE 22 (2016), https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf.

[32] MAEVE DUGGAN, ONLINE HARASSMENT 2017, PEW RES. CENTER 3 (2017), https://www.pewinternet.org/wp-content/uploads/sites/9/2017/07/PI_2017.07.11_Online-Harassment_FINAL.pdf; *see also* LENHART, *supra* note 31 ("47% of American internet users have experienced any of these 20 types of digital harassment.").

[33] DUGGAN, *supra* note 32 at 47 – 54; *see also Dylan E. Penza, The Unstoppable Intrusion: The Unique Effect of Online Harassment and What the United States can Ascertain from Other Countries' Attempts to Prevent It*, 51 CORNELL INT'L L.J. 297, 308 (2018).

[34] *See* Colleen M. Koch, *To Catch To Catch a Catfish: A Statutory Solution for Victims of Online Impersonation*, 88 UNIVERSITY OF COLORADO LAW REVIEW 234, 245 (2016).

[35] *See id.*

[36] *See id.* at 242.

workplace for sex."[37] According to the lawsuit, hundreds of interested individuals contacted Herrick and some physically sought him out.[38] Herrick reported the impersonation to Grindr approximately 100 times but Grindr did not respond, "other than to send an automated, form response."[39]

Herrick ultimately sued Grindr to hold the company liable for its failure to "incorporate certain safety features that could prevent impersonating profiles."[40] In particular, Herrick argued that Grindr did "not use 'proven and common image recognition or duplicate-detection software,' which could be used to search for profiles using Herrick's picture."[41] Furthermore, "Grindr d[id] not have the ability to search for IP addresses, MAC addresses, and ICC numbers or block the use of spoofing, proxies, and virtual private networks (VPNs), all of which might prevent new impersonating accounts."[42] Finally, Grindr did not utilize "a technique called 'geofencing' to determine when an impersonating account is associated either with Herrick's address or the address of his former boyfriend."[43]

Finding that Grindr was protected by Section 230, the United States District Court in New York granted Grindr's motion to dismiss. The Court added that, "[t]o the extent Herrick has identified a defect in Grindr's design or manufacture or a failure to war, it is inextricably related to Grindr's role in editing or removing offensive content – precisely the role for which Section 230 provides immunity."[44] On appeal, the United States Court of Appeals upheld the lower court's decision, affirming that, "manufacturing and design defects claim seek to hold Grindr liable for its failure to combat or remove offensive third-party content, and are barred by Section 230."[45]

With websites and social media platforms immune from liability under Section 230, victims of online impersonation, such as Herrick, cannot hold the websites and platforms accountable for their own conduct in perpetuating or exacerbating the abuse. More importantly, with Section 230 immunity, websites and platforms lack the incentives to ensure protocols are incorporated into their products and services to protect against future impersonation.[46] Accordingly, Section 230 should be amended to condition immunity on websites following regulations to be established to combat online impersonation. The regulations should be transparent and scalable to provide flexibility to websites based upon their size and resources.

---

[37] *Herrick v. Grindr, LLC*, 306 F. Supp. 3d 579, 584 (2018).
[38] *See id.*
[39] Id. at 585.
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Herrick*, 306 F. Supp. 3d at 585.
[44] *Id.* at 588.
[45] *Herrick v. Grindr, LLC*, No. 18-396, 2019 WL 1384092 *3 (2d Cir. Mar. 27, 2019).
[46] *See* Koch, *supra* note 34 at 251-252.

Individuals and businesses should have the right to be protected from online impersonation and websites should be required to incorporate protocols to prevent such abuse.

Nonconsensual Pornography

In 2016, the Data and Society Research Institute published a report on nonconsensual image sharing, which it defined as "when someone shows, sends, or posts nude or nearly nude photos or videos of someone else without the consent of the person pictured."[47] Nonconsensual image sharing is commonly referred to as "revenge porn."[48]

According to the report, "[r]oughly 3% of all online Americans have had someone threaten to post nude or nearly nude photos or videos of them online to hurt or embarrass them, and 2% of online Americans have had someone actually post a photo of them online without their permission."[49] Accordingly, "4% of internet users-one in 25 online Americans-have either had sensitive images posted without their permission or had someone threaten to post photos of them."[50] Notably, "[o]ne in 10 women under the age of 30 have experienced threats of nonconsensual image sharing, a much higher rate than either older women or older and younger men."[51]

In 2019, Rep. Jackie Speier introduced a bill in Congress that would criminalize revenge porn.[52] Nevertheless, with the absence of current legislation to address nonconsensual pornography, over forty-five states have enacted some form of legislation to address the issue.[53] In addition to federal legislation to criminalize the posting of revenge porn, Congress should empower administrative regulations to govern the removal of such content when posted. Many victims face severe obstacles in seeking the removal of nonconsensual images. To empower victims, Congress could require websites remove nonconsensual images as a condition of receiving Section 230 immunity.

Doxing

Doxing is when personal information is purposely posted on the Internet to inflict harm.[54] On the Internet, innocuous information, such as a person's phone number, email address or

---

[47] AMANDA LENHART, ET. AL., NONCONSENSUAL IMAGE SHARING: ONE IN 25 AMERICANS HAS BEEN A VICTIM OF "REVENGE PORN", DATA & SOCIETY RESEARCH INSTITUTE 3 (2016).
[48] *Id.*
[49] *Id.* at 4.
[50] *Id.*
[51] *Id.* at 5.
[52] The Stopping Harmful Image Exploitation and Limiting Distribution Act of 2019 (the "SHIELD Act"), H.R. 2896, 116 Cong. (2019).
[53] *Revenge Porn Laws*, CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/revenge-porn-laws/
[54] *See* PENZA, *supra* note 33 at 303-304; *see also* Victoria McIntyre, *"Do(x) You Really Want to Hurt Me?": Adapting IIED as a Solution to Doxing by Reshaping Intent*, 19 TUL. J. TECH. & INTELL. PROP. 111, 113 (2016).

home address can become weaponized. Combating doxing requires a multi-prong strategy that includes amending Section 230, regulating data brokers and limiting accessibility to personal information.

California prevents state or local agencies from publishing on the Internet the address and telephone numbers of "elected or appointed officials", which includes law enforcement officers, judges, prosecutors and other public officials.[55] The law further restricts any person, business or association to post the home address or telephone number of "any elected or appointed official if that official has made a written demand of that person, business, or association not to disclose his or her home address or telephone number."[56] Section 230 should likewise be amended to require websites to remove personal information, including a person's home address, phone number and email address upon request. If a website failed to honor a takedown request, the website should be subject to liability if a person suffered any damage as a result of the website's inaction.

Currently, there is no federal law requiring websites to remove personal identifying information upon request. Generally, websites will remove social security numbers, bank account numbers, credit card numbers and personal medical records.[57] That being said, dates of birth, addresses and telephone numbers will typically not be removed.[58] Individuals should have greater control over their personal information and have the option to remove such content. At the least, it should be up to a regulatory body, not the websites themselves, to determine which forms of personal information should be subject to removal.

As a supplement to amending Section 230, Congress needs to closely examine the data broker industry in general. Data brokers often collect, aggregate and sell personal information without an individual's knowledge or consent.[59] It is troubling that personal information collected by data brokers can ultimately be used by others for various nefarious purposes, including by businesses to make discriminatory housing, lending and employment decisions.[60] Americans require greater authority over their personal information, including possessing the ability to easily opt-out from or delete information held by data brokers through an online portal.

---

[55] California Government Code § 6254.21.
[56] *Id.* at § 6554.21(c)(1).
[57] *See, e.g.*, REMOVAL POLICIES, GOOGLE SEARCH HELP, https://support.google.com/websearch/answer/2744324?hl=en (last visited April 23, 2019); REMOVE SEARCH RESULTS FROM YAHOO SEARCH, YAHOO! HELP, https://help.yahoo.com/kb/SLN4530.html (last visited April 23, 2019).
[58] *See, e.g.*, REMOVAL POLICIES, GOOGLE SEARCH HELP, https://support.google.com/websearch/answer/2744324?hl=en (last visited April 23, 2019).
[59] Steven Melendez and Alex Pasternack, *Here are the Data Brokers Quietly Buying and Selling Your Personal Information*, FASTCOMPANY.COM (March 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.
[60] *See* PASQUALE, *supra* note 27 at 21.

In a recent Op-Ed for Time Magazine, Apple's CEO, Tim Cook, addressed the need to regulate data brokers. Mr. Cook wrote:

> Meaningful, comprehensive federal privacy legislation should not only aim to put consumers in control of their data, it should also shine a light on actors trafficking in your data behind the scenes. Some state laws are looking to accomplish just that, but right now there is no federal standard protecting Americans from these practices. That's what we believe the Federal Trade Commission should establish a data-broker clearinghouse, requiring all data brokers to register, enabling consumers to track the transactions that have bundled and sold their data from place to place, and giving users the power to delete their data on demand, freely, easily and online, once and for all.[61]

Allowing individuals to remove their personal information from the Internet, quickly, easily and in one centralized portal would minimize the personal information about a person that could be accessed for malicious purposes. The National Do Not Call Registry could serve as a model for a Do Not Collect Data Registry.[62] However, to hopefully make a "Do Not Collect Data Registry" more successful, search engines, such as Google, should also face liability for indexing entities in violation of the Registry.

On a broad level to further combat online harassment, Congress should pass a version of the Online Safety Modernization Act of 2017, a bill that was introduced in the previous Congress by Representative Katherine Clark.[63] Among other provisions, the bill criminalized additional forms of online abuse, including sextortion, swatting and doxing and provided additional funding in grants to state and local law enforcement to combat cybercrimes.[64] As noted in the Pew survey, "[a] plurality of U.S. adults (43%) say that law enforcement does not take incidents of online harassment seriously enough."[65] Frustration with law enforcement is a common theme among victims of online abuse and law enforcement needs additional resources to ensure that criminal behavior on the Internet is properly investigated and prosecuted.[66]

---

[61] Tim Cook, *You Deserve Privacy Online. Here's How You Could Actually Get it*, TIME.COM (Jan. 16, 2019), http://time.com/collection-post/5502591/tim-cook-data-privacy/.

[62] *National Do Not Call Registry*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry (last visited April 23, 2019).

[63] Online Safety Modernization Act of 2017, H.R. 3067, 115th Cong. (2017).

[64] *See id.*

[65] Duggan, *supra* note 32 at 48.

[66] *See generally* DANIELLE CITRON, HATE CRIMES IN CYBERSPACE 20, 23, 83 – 90, 144 - 145 (Harvard University Press 2014); *see also* Penza, *supra* note 33 at 316; *see also* McIntyre, *supra* note 34 at 123.

Living in the Information Age has resulted in our personal information being more vulnerable than ever. In order to ensure that our personal information is not used for abusive ends, our laws need to change to provide individuals greater control over their own information.

PROCEDURAL-BASED REFORMS

Victims of online abuse are often victimized twice, first by the abusive content itself and second, by a system that makes addressing the abuse far too complicated, time-consuming and expensive. In *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, then Chief Judge Kozinski noted that, "[t]he Communications Decency Act was not meant to create a lawless no-man's-land on the Internet."[67] However, that is what the Internet has become without the threat of liability. Baseline procedural protocols are necessary for websites and immunity under Section 230 should be conditioned upon adherence to such protocols.

Court Orders

According to the Pew survey, "[a]bout one-quarter of all adults (26%) have had untrue information about them posted online, most commonly about their character or reputation (17%). Half (49%) of those who had untrue information posted about them tried to get the inaccurate information removed or corrected."[68] Of those individuals who sought the removal or correction of inaccurate content, 28% were ultimately unsuccessful in their efforts.[69] Moreover, another 33% found the process of seeking to remove or correct inaccurate content to be difficult.[70] It should not be so difficult to remove inaccurate or damaging information from the Internet.

As it currently stands, Section 230 can serve as a roadblock for individuals to secure the removal of content deemed defamatory by a court of law. In *Hassell v. Bird*, the plaintiff sued the poster of an online review on Yelp.com.[71] After Hassell obtained a default judgment that ordered Yelp to remove the defamatory review, Yelp's counsel, "wrote Hassell a letter that identified several perceived deficiencies with the judgment and removal order."[72] Moreover, Yelp indicated that it "sees no reason at this time to remove the reviews at issue."[73] Yelp challenged the order that compelled it to remove the review on the basis of that the order, "violated the company's due process rights, exceeded the scope of relief requested in the complaint, and was barred by section 230."[74]

---

[67] *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1164 (9th Cir. 2008).
[68] Duggan, *supra* note 32 at 11.
[69] *Id.* at 58.
[70] *Id.*
[71] *Hassell v. Bird*, 420 P.3d 776 (Cal. 2018), *cert. denied*, *Hassel v. Yelp, Inc.*, 139 S.Ct. 940 (2019).
[72] *Id.* at 781.
[73] *Id.*
[74] *Id.*

After the California Court of Appeals upheld the injunction issued against Yelp, the company appealed to the California Supreme Court.[75] The Supreme Court sided with Yelp on the basis of Section 230, finding:

> With the removal order, plaintiffs seek to overrule Yelp's decision to publish the three challenged reviews. Where, as here, an Internet intermediary's relevant conduct in a defamation case goes no further than the mere act of publication – including a refusal to depublish upon demand, after a subsequent finding that the published content is libelous – section 230 prohibits this kind of directive.[76]

By virtue of the expansive immunity afforded under the CDA, websites can ignore court orders without penalty. This legal loophole was not what Section 230 intended to protect. To address this issue, Section 230 immunity should be conditioned upon websites honoring court orders for the removal of content. If a website were to ignore a court's order, immunity under Section 230 should be lifted and the website itself should become subject to publisher liability.

In considering the importance of court orders vis-à-vis Section 230 of the CDA, Congress should examine the policies of some websites in particular who explicitly refuse to honor court orders. Notably, RipoffReport.com will not remove reports, even with a court order, but only "redact" content found defamatory.[77] Moreover, RipoffReport.com will not consider "default judgments or stipulated orders that does not consider evidence."[78] Once a post is made on RipoffReport.com, according to the website, the post cannot be altered by the original poster.[79] Therefore, an order for the removal of content issued to the original poster of the content may not achieve the desired result and the pages containing defamatory content may continue to rank prominently on search engines, thus frustrating the original purpose of seeking and obtaining the judicial relief. Simply, victims of online defamation should not be subject to the whims and policies of varying websites and Congress should require that court orders are enforced.

Anonymity

Anonymous speech has been a part of the American story since the country's beginning. Famously, the Federalist Papers written by Alexander Hamilton, James Madison and John Jay were published in 1787 and 1787 under the pseudonym Publius.[80] The United States Supreme

---

[75] *See id.* at 783.
[76] *Id.* at 789.
[77] *Ripoff Report Legal Department*, RIPOFF REPORT.COM, https://www.ripoffreport.com/legal (last visited April 6, 2019); *see also* Lori A. Roberts, *Brawling with the Consumer Review Site Bully*, 84 U. CIN. L. REV. 633, 642 (2016)
[78] *Id.*
[79] *See id.*
[80] *The Federalist Papers*, CONGRESS.GOV (last visited April 28, 2019), https://www.congress.gov/resources/display/content/The+Federalist+Papers.

Court continues to protect anonymous speech, declaring in *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995), that speaking anonymously remains "an aspect of the freedom of speech protected by the First Amendment." The right to anonymous speech, however, is not the right to untraceable speech.

While the ability to speak anonymously remains valued, anonymous speakers may be unmasked under certain circumstances, including when they defame another person or business. In *Dendrite International, Inc. v. Doe, No. 3*, a New Jersey appellate court set forth a test for the allowance of discovery to unmask an anonymous speaker.[81]

Under the test, a plaintiff must first "undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure."[82] Second, the plaintiff is required "to identify and set forth the exact statements purportedly made by each anonymous poster than plaintiff alleges constitutes actionable speech."[83] Next, "[t]he complaint and all information provided to the court should be carefully reviewed to determine whether plaintiff has set forth a prima facie cause of action against the fictitiously-named anonymous defendants."[84] Finally, "the plaintiff must produce sufficient evidence supporting each element of its cause of action, on a prima facie basis, prior to a court ordering the disclosure of the identity of the unnamed defendant."[85]

The process to unmask an anonymous speaker is burdensome and is intended to be so. Yet, if an anonymous speaker on the Internet utilizes technology to mask their identifying information or if a website fails to retain records pertaining to online posters, "the right of the plaintiff to protect its proprietary interests and reputation," will be unavailable.[86] The problem created by anonymous speech on the Internet is significant. According to the 2017 Pew survey, "[r]oughly half of those who have been harassed online (54%) say their most recent incident involved a stranger and/or someone whose real identity they did not know."[87]

Plaintiffs must have the ability to unmask anonymous users if permitted by a court.[88] To effectuate this objective, websites need to maintain IP records to cover the statutory period for defamation and incorporate protocols to ensure the identity of a poster can be obtained. If a website does not maintain such records, thwarts the ability of plaintiffs to obtain identifying information or allows for anonymity as a service to its users, the website itself should become

---

[81] *Dentrite International, Inc. v. Doe, No. 3*, 342 N.J. Super. 134, 141 (App. Div. 2001).
[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] Duggan, *supra* note 32 at 11.
[88] *See* Roberts, *supra* note 77 at 636 ("Legal recourse for claims of defamation against an online reviewer is generally futile because reviewers post comments anonymously and unmasking the identify [sic] of an anonymous reviewer is a circular-often losing-battle with state procedures that require a business to prove the statement is false, without knowing the complainer's identity.").

liable as a publisher and it should lose its Section 230 immunity.[89] Websites should have the right to embrace anonymity enhancing technology but not at the cost of preventing individuals and businesses from having the ability to unmask anonymous speakers on the Internet.

Subpoenas/Out of Country Entities

The procedure to issue a subpoena to unmask an anonymous speaker is dependent upon the court where the underlying lawsuit is filed. Subpoenas in federal court are relatively straightforward and can be served using a standardized federal form.[90] State court subpoenas, on the other hand, are more complicated and attorneys and pro se litigants must follow the rules in both the home jurisdiction of the case and the foreign jurisdiction where the subpoena is to be issued.

RipoffReport.com is a website located in Arizona.[91] Its website indicates that subpoenas to be issued for the unmasking of its users must follow Arizona's rules, which require the subpoena be issued from an Arizona court.[92] In addition, among other requirements, Ripoffreport.com requires the subpoena be issued to the legal name of the website's parent, the subpoena must be personally served on its statutory agent and the subpoena must be accompanied with a "$150.00 processing fee."[93] For individuals or businesses who obtained permission to issue a subpoena to an anonymous online poster of content, the state subpoena process can be unduly costly and burdensome.

The cross-jurisdictional nature of the Internet lends itself to rules that apply consistently and broadly. For this reason, a federal court division that would handle online defamation matters, as already referenced, would be beneficial.

Despite the cost and procedural hurdles created by state subpoenas, at the least, entities within the United States are subject to its jurisdiction. Obtaining information from international companies or companies that do not have registrar contact information prove problematic. In such cases, United States courts have limited power to compel the turnover of information from these websites.

The reputations of individuals and businesses should not be dependent upon where a website is hosted or the level of a website's cooperation. Websites, regardless of jurisdiction, rely upon search engines. To ensure that websites are answerable to subpoena requests, Section 230 should be amended to require that all websites provide a United States address for service of

---

[89] *See, e.g.*, *Home*, CHEATERLAND.COM (last visit March 13, 2019) ("If you prefer not to create an account, you [sic] post would be anonymous.").
[90] *See Form AO 88B, Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action*, USCOURTS.GOV, available at https://www.uscourts.gov/sites/default/files/ao088b.pdf.
[91] *Legal*, RIPOFF.COM (last visited April 28, 2019), https://www.ripoffreport.com/legal.
[92] *Id.*
[93] *Id.*

process prominently in a privacy policy. Failure to include such an address and to respond to subpoenas pursuant to a streamlined process could result in such website losing its Section 230 immunity. Moreover, search engines should also be held responsible, upon notice, for indexing websites which fail to provide an address for service of process or which refuse to respond to subpoena requests.

CONCLUSION

Section 230 of the Communications Decency Act provides websites, social media platforms and search engines, "power without responsibility."[94] Under the current regulatory framework, the law makes no distinction between Internet companies who act as Good, Bad or Indifferent Samaritans. It would be reasonable, however, to demand more from Internet companies in return for their publisher immunity, including requiring them to comply with rules and regulations intended to provide greater powers to online abuse victims.

In *Fair Hous. Council v. Roommates.com, LLC*, 521 F. 3d 1157, 1175 (2008), then Chief Judge Kozinksi remarked that, "the Internet has outgrown its swaddling clothes and no longer needs to be so gently coddled." Amending Section 230 to deal with specific abusive content and procedural impediments will not destroy the social media industry and the Internet itself. Instead, amending the twenty-six words that created the Internet would save the Internet from falling deeper into a seemingly bottomless cesspool of harassment and abuse.[95]

To be clear, this paper is not recommending conditioning immunity to address online hate, fake news, deep fakes and other problems plaguing the Internet, of which there are many. While these issues pose serious threats to American democracy and to maintaining a civil society, establishing specific protocols to address such abuses without infringing upon free expression and constitutional protections would be difficult and constitutionally complicated. The complexities of legislating such issues should not stand in the way of conditioning Section 230 in those areas where defined standards of conduct can be implemented.[96]

---

[94] Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986 (2008).

[95] *See* KOSSEFF, *supra* note 1.

[96] An important debate has begun around big tech (e.g., Google and Facebook) and whether they possess too much power. *See, e.g.*, Kevin Roose, *Can Social Media be Saved?*, NY TIMES (Mar. 28, 2018), https://www.nytimes.com/2018/03/28/technology/social-media-privacy.html; Kara Swisher, *Nancy Pelosi and Facebook's Dirty Tricks*, NY TIMES (May 26, 2019), https://www.nytimes.com/2019/05/26/opinion/nancy-pelosi-facebook-video.html, Chris Hughes, *It is Time to Break Up Facebook*, NY TIMES (May 9, 2019), https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html. In particular, concerns have been raised over their data collection efforts, algorithmic biases and moderation policies. These are important debates to have and big tech may require additional oversight to ensure accountability and further transparency. Ultimately, Section 230 may have a role to play in regulating these companies. However, issues associated with big tech do not

Simply, the time for Congress to reexamine Section 230 is now. Conditioning Section 230 immunity to incentivize online platforms to tackle the specific harms and procedural issues discussed in this paper will clearly not solve every problem associated with the Internet, but it would be a start and for this reason, it is worth trying.

negate the importance of addressing online harms and procedural problems that require immediate attention and which should receive bipartisan support.